ABSTRACT

The present invention is a method and apparatus for testing the random numbers generated by a random number generator in real time. As a series of random numbers are generated, a plurality of the last numbers are stored, then the stored random numbers are shifted by predetermined amounts to obtain a special kind of dot product of bit sequences between the stored random numbers and the shifted random numbers. The average autocorrelation values are computed each time a new random bit is generated. Thereafter, it is determined whether the generated random numbers are not sufficiently random by comparing the average autocorrelation values to predetermined acceptance ranges.